UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/706,829	11/12/2003	Kyung-Duck Seo	8836-205 (IB12086-US)	6940

22150 7590 04/21/2008

F. CHAU & ASSOCIATES, LLC
130 WOODBURY ROAD
WOODBURY, NY 11797

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
04/21/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/706,829	SEO, KYUNG-DUCK	
	Examiner	Art Unit	
	CARL COLIN	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 January 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *see att*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 1/31/2008 has been entered.

Response to Arguments

2. In communications filed on 1/31/2008, applicant amends claim 7, the following claims 1-14 are presented for examination.

2.1 Applicant's remarks, pages 6-10, filed on 1/31/2008, with respect to the rejection of claims 1-14 have been fully considered but they are moot in view of a new ground of rejection.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on 1/31/2008 was filed after the mailing date of the Final rejection on 11/28/2007. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 9-10 are rejected under 35 U.S.C. 102(b) as being anticipated by Non-Patent Literature NN83024931, IBM Technical Disclosure, hereafter **IBM TDB**, "Checking Data Encryption Engines", February 1, 1983, (page 4931 and figure, previously submitted).

As per claim 9, **IBM TDB** substantially discloses an encryption apparatus having a substantially uniform current pattern during cryptographic processes comprising: a first N-round DES device (element 1 of figure) producing a first current pattern during cryptographic process on a digital input data block based on an input of a set of encryption keys (see Disclosure Text and figure); and a second N-round DES device (element 2 of figure) producing a second current pattern during cryptographic process on an inverse of the digital input data block, based on an input of the set encryption keys in inverted form (see Disclosure Text and figure), wherein the first and second N-round DES devices perform a substantially simultaneous cryptographic conversion process and wherein the first and second current patterns are inverse patterns respectively (see Disclosure Text and figure).

As per claim 10, **IBM TDB** discloses using implementing data encryption standard (DES) to perform the operations that meets the recitation of wherein the first and second N-round DES devices perform a cryptographic conversion process according to a DES algorithm, respectively (see Disclosure Text).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-4, 6-8, 11-12, and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Non-Patent Literature NN83024931, IBM Technical Disclosure, hereafter **IBM TDB**, "Checking Data Encryption Engines", February 1, 1983, (page 4931 and figure).

As per claim 1, **IBM TDB** substantially discloses an encryption apparatus comprising: a first N-round DES device (element 1 of figure) for cryptographically converting a digital input data block into a first digital output data block nonlinearly, based on an input of a set of

encryption keys (see figure); and a second N-round DES device (element 2 of figure) for cryptographically converting the inverted digital input data block into a second digital output data block nonlinearly, based on an input of the set of inverted encryption keys (see fig. 1), wherein the first and second N-round DES devices perform a substantially simultaneous cryptographic conversion process (see fig. 1 with description on Disclosure Text). **IBM TDB** discloses receiving the inverted digital input data block and receiving the inverted set of encryption keys but does not explicitly disclose a means for inverting them. It is implicit that a means for complimenting the inputs was used or would have been used by one of ordinary skill in the art so as to produce inverted inputs. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus as shown in the figure to provide means for inverting the digital input data block and inverting the set of encryption keys as suggested by **IBM TDB** so as to produce inverted data and key to be inputted as shown in the figure.

As per claim 7, **IBM TDB** substantially discloses a method of cryptographically converting digital input data comprising the steps of: cryptographically converting substantially simultaneously a digital input data block into a first digital output data block nonlinearly, based on an input of a set of encryption keys (see Disclosure Text and figure) and an inverse of the digital input data block into a second digital output data block nonlinearly, based on an inverse of the encryption keys (see Disclosure Text and figure). **IBM TDB** is silent about storing the outputs in a register. IBM TDB discloses using the outputs to perform operations (see Disclosure Text); Examiner takes official notice that storing results in a register is very well

known in the art and therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to store the results into a register so the results can be retrieved by an application to be applied to the XOR function.

As per claim 2, **IBM TDB** discloses using implementing data encryption standard (DES) to perform the operations that meets the recitation of wherein the first and second N-round DES devices perform a cryptographic conversion process according to a DES algorithm, respectively (see Disclosure Text).

As per claims 3 and 11, **IBM TDB** discloses either one of the first and second digital output data blocks being used as an encryption data block (see Disclosure Text and figure). **IBM TDB** is silent about storing the results. IBM TDB discloses using the outputs to perform operations. Examiner takes official notice that storing results is very well known in the art and therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to store the results so the results can be retrieved by an application to be verified for error as suggested by **IBM TDB** (see Disclosure Text).

As per claims 4 and 12, **IBM TDB** discloses the limitation of further comprising a third input means for transferring the digital input data block to the first N-round DES device (see figure).

As per claims 6 and 14, **Sprunk** discloses a fourth input means for transferring the set of encryption keys to the first N-round DES device (see figure).

As per claim 8, **Sprunk** discloses wherein either one of the first and second digital output data blocks being used as an encryption data block (see Disclosure Text and figure).

6. **Claims 5 and 13** are rejected under 35 U.S.C. 103(a) as being unpatentable over Non-Patent Literature NN83024931, IBM Technical Disclosure, hereafter IBM TDB, "Checking Data Encryption Engines", February 1, 1983, (page 4931 and figure) in view of US Patent 4,803,725 to **Horne et al**.

As per claims 5 and 13, does not explicitly disclose generating keys based on permutation. **Horne et al** in an analogous art discloses encryption key block for receiving a key and generating the set of encryption keys based on a permutation of the key (see column 10, lines 17-43 and column 13, lines 20-35 and column 14, lines 13-16). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use permutation so as to vary the keys and make them less susceptible to attacks as suggested by **Horne et al** (see column 2, lines 52-63).

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the prior art discloses many of the claimed features such as conversion of input to output with inverse transformation. (See PTO-form 892).

7.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to CARL COLIN whose telephone number is (571)272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Carl Colin/
Examiner, Art Unit 2136
April 15, 2008